In the Claims

No claims have been amended.

Please add new claims 21-35 as shown herein.

Claims 1-35 are pending and are listed following:

1. **(original)** In a computer system including at least one client computer coupled by a communications network to a secure storage facility located remotely to the client computer, a method of accessing a dedicated data storage unit, the data storage unit for storing data files associated with a user identification code in a secure environment, the method comprising the following steps:

initiating a request for accessing a dedicated data storage unit, the request specifying at least a remotely located secure storage facility containing the dedicated data storage unit and a user identification code, the secure storage facility associated with an address on a communications network;

in response to the request, automatically connecting to the remote secure storage facility at the associated address;

transmitting the request to the remotely located secure storage facility;

identifying the dedicated data storage unit associated with the specified user identification code; and

granting access to the identified dedicated data storage unit.

2. **(original)** The method as in Claim 1 wherein the step of granting access includes granting access to the identified dedicated storage unit in accordance with pre-existing instructions associated with the specified user identification code.

3. **(original)** The method as in Claim 1 wherein the request further specifies a processor identification code associated with a client computer, the step of identifying the dedicated data storage unit including identifying the dedicated data storage unit associated with both the specified user identification code and the specified processor identification code.

4. **(original)** The method as in Claim 1 including the further step of displaying to a user a directory of data files stored in the dedicated data storage unit.

A14

5. **(original)** The method as in Claim 4 including the further steps of:

selecting a data file from the displayed directory of data files; and

transmitting the selected data file to a client computer associated with the request.

6. **(original)** The method as in Claim 1 wherein each data file stored in the dedicated data storage unit has a predetermined security level assigned thereto, each data file being encrypted in accordance with its assigned security level.

7. **(original)** The method as in Claim 1 wherein the request further specifies at least one data file stored on the identified dedicated data storage unit, the method further comprising the step of transmitting the specified at least one data file to a client computer associated with the request.

8. (original) The method as in Claim 1 wherein each data file stored in the dedicated data storage unit is assigned a reference identification number by the secure storage facility at the time each data file is initially stored in the dedicated data storage unit.

9. (original) The method as in Claim 8 wherein each data file stored in the dedicated data storage unit is assigned a new reference identification number by the secure storage facility each time the data file is accessed by a user after being initially stored in the dedicated data storage unit.

A16

10. (original) The method as in Claim 1 including the further steps of:

storing one or more data files in the dedicated data storage unit after access has been granted; and

encrypting the data in the one or more data files in accordance with a user assigned security level associated with each data file to be stored.

11. (original) The method as in Claim 10 wherein the step of encrypting the data includes the step of encrypting the data at the secure storage facility prior to storing the one or more data files in the dedicated data storage unit.

12. (original) The method as in Claim 11 wherein the step of encrypting the data includes the step of encrypting the data at a client computer associated with the request prior to storing the one or more data files in the dedicated data storage unit.

13. **(original)** In a computer system including at least one client computer coupled by a communications network to a secure storage facility located remotely to the client computer, the remote secure storage facility identified by an address on the communications network and including at least one dedicated data storage unit for storing data files associated with a user identification code in a secure environment, encryption/decryption means and processor means, the remote secure storage facility adapted to allow access to the at least one dedicated data storage unit in accordance with a set of pre-existing instructions, apparatus for accessing the at least one data storage media such that the remote secure storage facility is transparent to a client computer, the apparatus comprising:

a logical data storage peripheral coupled to a client computer, the logical data storage peripheral associated with a remote secure storage facility; and

a controller associated with the logical data storage peripheral and storing the address on the communications network of at least one remote secure storage facility, the controller including machine executed means for:

receiving a request from a user on the client computer to access the logical data storage peripheral, the request specifying at least the logical data storage peripheral and a user identification code;

determining the address of the specified secure storage facility;

automatically connecting to the remote secure storage facility;

transmitting the access request to the remote secure storage facility; and

when access to a dedicated data storage unit associated with the specified user identification code has been granted, providing access to the dedicated data storage unit by routing communications between the client computer and the remote secure storage facility, the client computer unaware it is in communication with the remote secure storage facility.

14. (original) Apparatus as in Claim 13 further comprising encryption and decryption means for encrypting data files to be stored in a dedicated data storage unit and decrypting data files retrieved from a dedicated data storage unit.

A16

15. (original) Apparatus as in Claim 14 wherein a data file to be stored in the dedicated data storage unit associated with a user identification code is encrypted in accordance with a user assigned security level.

16. (original) Apparatus as in Claim 13 further comprising memory means for storing at least one directory, each directory containing a listing of data files stored in a dedicated data storage unit.

17. (original) A secure storage facility having an address on a communications network and adapted for communication with other devices on the communications network, the secure storage facility comprising:

one or more dedicated data storage units for storing data files in a secure environment, each of the dedicated data storage units identified by at least one user identification code; and

a processor coupled to each of the dedicated data storage units, the processor including machine executed means for:

A16

receiving an access request from a user on a remotely located client computer, the access request specifying at least a user identification code;

identifying a dedicated data storage unit associated with the specified user identification code; and

granting access to the identified dedicated data storage unit in accordance with a set of instructions associated with the specified user identification code.

18. (original) A secure storage facility as in Claim 17 further comprising encryption and decryption means for encrypting and decrypting data files associated with a user identification code in accordance with the set of instructions associated with the user identification code.

19. (original) A secure storage facility as in Claim 18 wherein a data file to be stored in the dedicated data storage unit associated with a user identification code is encrypted in accordance with a user assigned security level.

20. (original) A secure storage facility as in Claim 17 wherein the set of instructions associated with a user identification code specifies read-only, write-only or read/write access to data files stored in the dedicated data storage unit associated with that user identification code.

Please add new claims 21-35 as follows:

A6

21. (new) A secure data storage system, comprising:

a communications network address configured to identify the secure data storage system to a computing device communicatively coupled to the secure data storage system via the communications network;

a dedicated data storage unit configured to maintain data files generated by the computing device, the dedicated data storage unit identified by an identification code corresponding to the computing device; and

a processing component configured to receive and process a request to access the dedicated data storage unit, the request specifying the communications network address, the identification code, and a data file maintained with the dedicated data storage unit.

22. (new) A secure data storage system as recited in claim 21, wherein the identification code includes a processor identification code corresponding to the computing device.

23. (new) A secure data storage system as recited in claim 21, wherein the identification code includes a user identification code and a processor identification code corresponding to the computing device.

24. **(new)** A secure data storage system as recited in claim 21, wherein the processing component is further configured to grant access to the dedicated data storage unit in accordance with access instructions associated with the identification code.

25. **(new)** A secure data storage system as recited in claim 21, wherein the processing component is further configured to encrypt the data files in accordance with a security level associated with the identification code.

26. **(new)** A computing device, comprising:

a logical data storage peripheral corresponding to a remote secure data storage system that includes a dedicated data storage unit configured to maintain data files generated by the computing device, the dedicated data storage unit identified by an identification code corresponding to the computing device;

a controller configured to receive a request to access the logical data storage peripheral, the request specifying the logical data storage peripheral, the identification code, and a data file maintained with the dedicated data storage unit; and

the controller further configured to communicatively couple the computing device to the remote secure data storage system and communicate the request to access the logical data storage peripheral to the remote secure data storage system.

27. **(new)** A computing device as recited in claim 26, further comprising a processor configured to execute the controller, and wherein the identification code includes a processor identification code corresponding to the computing device.

28. **(new)** A computing device as recited in claim 26, further comprising a processor configured to execute the controller, and wherein the identification code includes a user identification code and a processor identification code corresponding to the computing device.

A16

29. **(new)** A method, comprising:

maintaining data files with a dedicated data storage unit that is identified by an identification code corresponding to a computing device, the dedicated data storage unit having an associated communications network address;

receiving a request to access the dedicated data storage unit, the request specifying the communications network address, the identification code, and a data file maintained with the dedicated data storage unit; and

granting access for the computing device to access the dedicated data storage unit in accordance with access instructions associated with the identification code.

30. **(new)** A method as recited in claim 29, further comprising generating the identification code to include a processor identification code corresponding to the computing device.

31. **(new)** A method as recited in claim 29, further comprising generating the identification code to include a user identification code and a processor identification code corresponding to the computing device.

32. **(new)** A method as recited in claim 29, further comprising encrypting the data files in accordance with a security level associated with the identification code.

A16

33. **(new)** A method, comprising:

generating a request to access a logical data storage peripheral that corresponds to a remote secure data storage system which includes a dedicated data storage unit to maintain data files generated by a computing device, the dedicated data storage unit identifiable by an identification code that corresponds to the computing device;

receiving the request to access the logical data storage peripheral, the request specifying the logical data storage peripheral, the identification code, and a data file maintained with the dedicated data storage unit; and

communicatively coupling the computing device to the remote secure data storage system; and

communicating the request to access the logical data storage peripheral to the remote secure data storage system.

34. **(new)** A method as recited in claim 33, further comprising generating the identification code to include a processor identification code corresponding to the computing device.

35. **(new)** A method as recited in claim 33, further comprising generating the identification code to include a user identification code and a processor identification code corresponding to the computing device.

A16